EC-2000-007
III-A-008

Architecture Design For Electronic Submission of Discharge Monitoring Reports

Prepared by: Ralph Berwanger

Prepared on: April 21, 1999

Discharge Monitoring Report (DMR) Submission using electronic processing

Logistics Management Institute recommends the following architecture for electronic DMR submission. The recommendation is based on an analysis of current and emerging technologies, EPA policy on DMR submission, technical and financial burdens that must be assumed by organizations submitting DMRs, and non-repudiation issues. The recommendation is sufficiently robust to support enterprises with mature electronic data interchange (EDI) capabilities and small enterprises with basic Internet connectivity.

LMI

The architecture is built around the Sterling GENTRAN Web Suite. This product supports web-based interactions or traditional ANSI X12 data interchanges. The Web Suite product limits the environment to those organizations that use Microsoft Windows® operating systems (Windows® 95, Windows® 98, and Windows® NT). UNIX and Mac users cannot interact with Web Suite. While this limitation is acknowledged, the proposed architecture will service a large portion of the community submitting DMR.

Figure 1- Basic Architecture

The proposed architecture imposes minimal financial burden on organizations that electronically submit DMRs. Organizations possessing traditional EDI capabilities must configure their operation to support the generation of a Report of Test Results (863) transaction set. The Government produced an implementation convention to assist this process. No additional software must be acquired. Any enterprise desiring to submit an electronic DMR must obtain and install a digitizing tablet on the workstation that will interact with the Internet. These devices are relatively inexpensive, unlike security software, security tokens, and the associated Public Key Infrastructure (PKI).

The proposed architecture provides sufficient assurances to the report submitters and the Government. Controls are defined to validate the authenticity of all reports submitted. The controls include the digitized signature of the report submitter, timestamps, and 'water marks' (hash value).

Description of the Architecture

The following description is supported by the information found in Figure 1 and Figure 2 of this document. For clarity, all references to the 'server' relate to actions performed by the Government. These are functions performed by the Web Suite server or processes running on the server. All users external to the server are referred to as the 'client.'

Establishing accounts with the Government. All clients must subscribe to the server. Figure 1, Steps 1 and 2, show the one-time subscription process. The client accesses the server and provides information about the client's organization. The server accepts the data and queues a response for the client. Internal policy is required regarding how the client is authenticated. However, assuming a policy exists, the server would forward the client a 'user identification' and 'passphrase.' Clients use the identification information to access the Web Suite applications.

Accessing DMR Processing Application. Clients, working from a Microsoft® Windows-based operating system through the Internet, use their Web browser to connect with the server and enter their user identification and passphrase. The server, running the Microsoft® Internet Information Server (IIS) authenticates the client. Next, the client is presented with the first screen of the DMR application. This process is captured in Figure 1, Steps 3 and 4.

Submitting DMR information. Two paths are used to submit DMR information to the server. The first path is reserved for clients providing information from a Web browser. These clients will enter the information directly into a form displayed on their Web browser. The Sterling GENTRAN Web Suite tool permits clients to produce the entire DMR on the client's browser and submit the report to the server as an ANSI X12 compliant transaction set. The second path is for clients submitting DMRs from an EDI translation facility. These clients may submit their reports using standard TCP/IP connections or value-added networks (VAN). Obviously, the TCP/IP connection would be less expensive than a VAN, but the client may already have VAN connection for use with other trading partners. Figure 2 details the internal process of the traditional EDI user. The interface between Figure 1 and Figure 2 is the client's call to the server following Step 5 in Figure 1.

Authenticating the DMR. All clients authenticate the DMR content by affixing a digitized signature to the report. The proposed architecture provides for the possibility that the individual entering DMR data is not the individual that will 'sign' the report. The architecture also anticipates the fact that clients providing traditional EDI input must access the Government's Web server after submitting the DMR to authenticate

the report. DMR submission is a two-step process: data entry and data authentication. Still, this solution is preferable to requiring clients to acquire additional security software, to develop applications at government expense, and to stand up a PKI. The signature process requires the client to prompt the server that a signature for a report is about to be generated. The server immediately annotates the time the signature function begins when the prompt from the client is received. The client then proceeds to create a signature using a digitizing device (digitizing tablet). Finally, the client submits the signature to the server. The server will compare the time of actual submission with the start-time of the process. Elapsed time for the process cannot exceed 30 minutes. Time periods exceeding 30 minutes are invalid, and the client is required to create another signature for the report. Figure 1, Step 6, represent this process.

Client verification of DMR submissions. The server provides the client a completed DMR. All information is based on information submitted by the client. In addition to the report information, the report displays the digitized signature of the client. The client is required to review and authenticate the information in the report. Since this information is presented on the client's Web browser, the client can print or save the report. Clients must enter their passphrase after reviewing the report. The server validates the passphrase entered by the client. After the passphrase is verified, the DMR information is stored in the Permit Compliance System (PCS) database. The server will place a final timestamp into the report prior to writing the information into PCS.

Client provided record copy of DMR. The server creates a duplicate copy of the report saved in PCS and forwards the report to the client. This report contains all the DMR data, the signature submitted by the client, and a 'watermark.' (hash value). The watermark will verify the authenticity of the DMR, if required.

Error Reporting and Feedback.

The basic architecture defined above does not describe the process for reporting errors to the client. Errors are classified into two categories: syntax errors and compliance errors.

Syntax errors violate rules defined in the ANSI X12 standard. The violations are errors in the data, where the submitted data does not conform to the data that was expected by the server. (For example: the server expected a numeric value and received a text value, the server expects a value less than ten and receives a double-digit value, or the server expects a defined number of iterations of a value and the client submits too few or too many values.) The server must notify the client if any of these errors occurs. The client submitting DMRs using their Web browser will receive immediate feedback from the server. The server will not permit the client to submit the report until the detected errors are corrected. Clients submitting DMR data using traditional EDI will receive syntax error reports in the form of Functional Acknowledgement (997) transaction sets. The 997 transaction set is automatically generated by the Sterling GENTRAN software and forwarded to the client.

Compliance errors are DMR errors that relate to regulatory issues. These errors would not be detected as syntax errors because they do not violate ANSI X12 rules. (For example: a submitted report may state that the concentration of a specific material discharged was 100 parts per 1000, but regulations require the concentrations shall not exceed 10 parts per 1000.) The basic architecture cannot support this level of compliance checking or error reporting. The architecture relies on processes resident in PCS to perform those checks. PCS would generate the error information. That information would be formatted into an Application Advice (824) transaction set, if the client was a user of traditional EDI. Clients who submit reports using their Web browser would have the error report posted to their account, on the server.